Mobile Systems and Security:

Technologies for Safe, Anywhere/Anytime Computing

Contents

Executive Summary

Two of today's biggest trends in corporate computing are in direct conflict.

The first trend is the rise of the mobile workforce. Affordable, high-performance mobile PCs have unchained employees from their desks, allowing them to get more work done wherever they go – at home, while traveling, on job sites and in hotels. Gartner Consulting estimates that business users with notebook computers who spend 20% or more of their time out of the office realize a minimum annual benefit of $34,560 due to improved productivity and efficiency. At the same time, the TCO of notebook computers has declined 30% from 1998 to 2001.[1]

It's no wonder that the number of mobile computers sold worldwide increased from 19.7 million in 1999 to 25.5 million in 2001 – a growth rate three times higher than desktop PC shipments. One in every four systems currently sold is a mobile PC. In the United States, 37 percent of professionals already use notebooks instead of desktops, and in Japan, the figure is 54 percent according to Fujitsu Siemens.[2]

The second trend is increasing security risks to corporate data, networks and equipment. According to Safeware, The Insurance Agency, 387,000 laptops were stolen in 2000, a 21 percent increase over the previous year.[3] The hardest hit industries are manufacturing, healthcare, government and others that employ large numbers of mobile workers traveling to multiple sites.[4]

Understanding the Risks

Notebooks can be lost or stolen; their Internet communications with headquarters can be intercepted; their wireless networking links can be eavesdropped – if users and IT managers don't take the necessary precautions.

The first thing people tend to worry about is loss of the equipment itself through theft or negligence. But the damages only get worse. Mobile PC users often go for days without connecting to the network, and are notoriously lax about backing up their data. A missing notebook takes a double toll on productivity – the time it originally took to create files and the time it takes to re-create those files because they are no longer available. And even if a current backup exists, there are other, unacceptable losses – such as the time it takes to configure a replacement system, or the opportunities that are lost when an employee is stranded on the road without the information needed to do business.

Then there's the potential value of that data to the thief. Stolen notebooks may contain trade secrets, legal contracts, payroll data and other information that puts the company at a competitive risk. When you consider that the hotspots for notebook theft include offices, airports, convention centers and hotels – places where competitors often cross paths – this risk is very real.

Even if the thief is a garden-variety thug rather than a competitor, there's a good chance the notebook will wind up in the hands of someone who enjoys causing others pain – and that may mean someone who will hack into your network if given the opportunity. When passwords and network software are stored on the notebook's hard drive, accessing the network can be far too simple.

The risks of data theft or network attack are further complicated by the rise of wireless networking, which is an increasingly important way for mobile workers to connect. With confidential information traveling through the air rather than over the wire, it's especially important to ensure that no one can intercept it.

Mobile Security Solutions and Intel's Role

Companies have much to gain – and potentially much to lose – by deploying mobile PCs and devices for their increasingly mobile workforce. So the question is how to eliminate the potential downside, making the mobile revolution a win across the board?

The answer is choosing and using the appropriate security technologies and procedures for:

- Platform security
- Data protection and system integrity
- Communications security

The good news is that Intel and other industry leaders are continuing to push mobile security technologies to the highest levels, helping mobile users protect their systems and data with the same confidence their desktop-bound colleagues enjoy.

From low-tech cable locks to high-tech wireless security initiatives, there are current and emerging technologies to protect physical platforms and data as well as the communications networks that keep mobile workers connected to the corporation. By analyzing the financial and competitive risks your business faces when it sends mobile workers out into the world, you can choose the appropriate technologies to maximize your Return on Security Investments (ROSI) and protect your business interests.

Read on to learn about current and emerging technologies designed to protect your mobile platforms, data and communications links from loss, theft, intrusion or attack.

Platform Security

Your first line of defense should always be to safeguard mobile platforms from theft of unauthorized access. While a notebook is under the authorized user's direct, physical control, there's little a thief or corporate spy can do. And there are effective measures you can take to protect systems and data even when they're separated from the user.

Cable locks. Like a bicycle lock, cable locks for mobile devices secure the device to a fixed object. And, like a bicycle lock, their effectiveness depends on how they are used. First and foremost, the notebook should be locked whenever the mobile PC is not in transit. It only takes a second to steal a notebook – so, for example, a simple trip to the hotel ice machine could be a disaster unless the PC is locked. And most notebook thefts are inside jobs, so it should be locked even while at the office.

Return on Security Investments: A ROSI Scenario

Spending money on security is always a tough sell to the company bean-counters. That's because there's no easy way to cost-justify it. Traditional ROI calculations project that spending "X" amount on technology will eventually return "Y" to the bottom line in increased sales or employee productivity. If "Y" is greater than "X," and if "eventually" falls within the horizon of the current business plan, then the technology expenditure is justified.

But when you're talking about security, "Y" doesn't come in the form of a tangible return. Instead, you spend money on security in order to prevent a loss. And there's no "eventually" about it – there's no horizon beyond which any loss is OK. So your cost justification ends up something like this: If we spend "X" amount on security, maybe we'll prevent loss of valuable equipment or company information, at some point. And if the investment is a good one, you'll never know what might have been lost.

Fortunately, researchers from Stanford, MIT's Sloan School of Management, and the @Stake security consultancy have created objective methods for calculating the Return on Security Investment, or ROSI. Their work demonstrates that the earlier a company introduces security analysis and engineering into its processes, the higher the ROSI. For example, by introducing security at various stages, companies achieve the following ROSI on average:

Intro Security At:	ROSI:
Design	21%
Implementation	15%
Testing	12%

@Stake Labs also claims that security can increase efficiency 3 percent or more when systems are configured correctly and unused processes are shut off to maximize security and performance.
For more information on @Stake's research and services, visit www.atstake.com.

(Source: "Coming up ROSI," CIO.com, October 26, 2001)

Furthermore, it must be locked correctly. This means knowing how to engage the lock in the receptacle on the notebook's case, and ensuring that the cable is attached to something solid and immovable.

Cables locks can be difficult or even impossible to use while on the road. And they can be cut by determined thieves using the right tools. For these reasons, it's often a good idea to use cable locks in combination with another security technique. Nevertheless, if it's used appropriately, consistently and correctly, a cable lock is usually sufficient to send a petty thief in search of an easier target.

Polarizing screen filters. These are simple, inexpensive devices that permit a direct line-of-sight view of the notebook's screen, but block the view from any other angle. This can help prevent an eavesdropper from accessing sensitive information by simply looking over the user's shoulder.

Motion detection systems. Notebooks can be equipped with alarms or notification systems that activate automatically when the device is moved or taken out of a specified area. These systems are most useful when the owner or another responsible party is nearby. For example, you might choose this approach to protect notebooks at your central office, so users can move about freely without constantly dealing with cable locks. Offsite, however, it's probably best not to depend solely upon an alarm system – just as it would be unwise to use a car alarm without locking the doors.

Some motion-detection systems can prevent the PC from booting until a code is entered to unlock it. If you're more concerned about the theft of corporate data than the machine itself, this type of system can be very effective – especially when combined with encryption of data on the hard drive.

Notebook-tracing software. Special software can be installed on the notebook that automatically notifies your company when a stolen machine is logged onto the Internet. The software can send information such as the IP address and phone number where the notebook is currently located, and also allow the authorized user to retrieve and/or erase sensitive files independent of the unauthorized user's control.

Some tracing software can even dial a phone number – for example, the police, a security service or your corporate headquarters – to deliver a message without the unauthorized user's knowledge. And tracing software can incorporate hard-drive encryption, rendering data useless until the notebook is recovered and returned to its owner.

Of course, tracing software does nothing to prevent the loss of equipment. And until the notebook is connected to the Internet, it provides no data protection. Nevertheless, tracing software can be a cost-effective, extra measure of protection that may thwart data theft or even aid in apprehending the criminal and returning the equipment.

What Intel is Doing about Platform Security

The end-user has primary responsibility for platform security, and it's the corporation's responsibility to train and enforce proper procedures for securing mobile PCs. Intel is doing everything it can to support corporations and users in this endeavor by making platform security as simple and reliable as possible.

One example is Intel's leadership within the Trusted Computing Platform Alliance* (TCPA). In partnership with other industry leaders including Compaq, Hewlett-Packard, IBM, Microsoft and more than 160 other companies, Intel is working through the TCPA to deliver hardware and operating system standards that maximize the level of trust users can have in their desktop and mobile PCs.

TCPA standards are all-inclusive, running the gamut from detecting and reporting evidence of tampering to sophisticated platform-identification policies. TCPA standards also support the other levels of security discussed later in this paper.

Data Protection and System Integrity

Almost always, the intellectual assets contained on a mobile PC's hard drive are more valuable than the physical asset of the PC itself. Although most companies can afford to budget for replacement of lost, stolen or damaged equipment, the loss of data is usually far more devastating.

These potential data losses can have three dimensions. First, there's the problem of wasted productivity when irreplaceable files become unrecoverable. If a notebook is stolen and pawned, for example, and current backups of the hard drive don't exist, you've lost all the time and effort that went into producing the files on it – as well as all the leverage those files could have had in producing new work in other areas. A single file can affect the work of dozens or even hundreds of employees, and the combined costs – although they don't show up on the books – are usually orders of magnitude worse than the cost of the lost PC itself.

Second, there's the problem of theft of proprietary information. If a notebook is stolen by or offered to a competitor, the information on it could cause incalculable damage to your company. This hazard also extends to transmissions between the notebook and corporate servers. When data is stolen from the hard drive or over the wire, anything is possible – from theft of product specifications to negative publicity to outright sabotage. It's just as important to control and protect the data that leaves the office on a notebook's hard drive as it is to control access to the corporate network.

Third, you need to protect the integrity of data and computing systems. A disreputable competitor doesn't necessarily need to steal your data to gain an advantage; simply destroying or altering your data can be almost as effective. And unfortunately, there are many tech-savvy vandals who are motivated to destroy data simply for the thrill of it. Mobile PCs are subject to attack by viruses, worms and other malicious programming, just like desktop PCs. Mobile PCs are even more vulnerable, however, because they're often left unattended. It can take only a few seconds for someone to introduce malicious programming, for example via a removable diskette.

There are several security schemes that can be used alone or in combination to prevent unauthorized access or destruction of data. These schemes fall into two general categories:

- Pre-boot authentication techniques require user identification before the operating system loads. These techniques can be executed as part of the BIOS upon initial power-up, and have the advantage of rendering the notebook completely useless to anyone but the authorized user.
- Post-boot authentication techniques allow the operating system to start up and the notebook to become functional, but prevent unauthorized access to sensitive data on the hard drive. Because these techniques are supported by the operating system, vendors can easily provide a wide variety of options – from affordable, software-only solutions to smart cards, biometric systems and more.

A variety of security techniques are available and emerging for both the pre- and post-boot environment, allowing you to choose the approach that best suits your particular risk exposure as well as your users' preferences. For the most sensitive corporate data, a combination of pre- and post-boot authentication methods can provide nearly unbreakable security. Pre- and post-boot implementations are available for all the following security technologies.

Biometric readers are sophisticated authentication devices which measure the unique physical characteristics of a user. For example, fingerprint readers can be incorporated into PC cards or directly onto the notebook itself, checking the user's unique fingerprint against a database of authorized users before the machine can be used.

Subsystems such as built-in PC cameras already exist – and others are rapidly emerging – that can easily be adapted to support fingerprint, face, voice and other biometric recognition technologies. Only a few years ago, these technologies were the stuff of science fiction. Today, they're often used in high-security buildings, and it won't be long before they're commonplace in notebook PCs that contain valuable corporate data.

Smart cards and USB tokens are another authentication technique, requiring the user to insert a card into a PC slot before logging on. This approach is similar to an ATM machine, which requires the user to prove his or her identity by producing a uniquely coded card and a matching personal identification number (PIN). As this form of authentication becomes commonplace, notebook designers will need to keep notebook form factors small while ensuring that cards are durable, easy to carry without losing, and easy to use.

User IDs and passwords can be used both as a simple form of authentication during the boot process, as well as a key for unlocking a data encryption scheme. This approach is widely used, and is familiar even to desktop workers. However, as any IT manager can attest, user IDs and passwords can easily be circumvented unless users protect them conscientiously. A password that's easy to guess, is written down, or is shared with others can be very easy for a motivated thief to steal. This danger is even more serious for mobile users who don't have the additional protection of a front-desk security guard.

Several other authentication devices – including iButton*, encoded key fobs, signature readers, infrared body-pattern readers, typometric analyzers, and more – provide a wealth of alternatives in addition to the authentication techniques described above.

Data encryption can be used on the hard drive and in data transmissions to make information unreadable until the user presents a security key that decodes it. The key can be presented explicitly (as in many third-party encryption solutions), or the entire process can be performed automatically and transparently (as in Windows* 2000 and Windows XP, for example). Encryption can be implemented as part of, or in addition to, any of the authentication methods described above, making it impossible to retrieve meaningful data even if the machine is successfully booted.

Data encryption can be very effective, as long as the user scrupulously protects the means of accessing the data. And of course, if the means of access are lost – for example, if a password is forgotten – the data becomes inaccessible even to the authorized user. Fortunately, today's best encryption implementations include mechanisms that allow you to recover data in the event the key is lost, and require you to set up the recovery steps before encrypting data.

What Intel is Doing about Data Security and System Integrity

Intel® Protected Access Architecture defines services that can be used to prevent unauthorized users from booting a mobile or desktop PC. IPAA does this by providing a common mechanism for computers to take advantage of new-user authentication technologies such as fingerprint recognition, smart cards, USB tokens and others. IPAA technology makes the contents of a PC useless to a thief, and simply knowing it's there can help deter theft in the first place. IPAA's ability to authenticate users works hand-in-hand with TCPA's ability to authenticate platforms, providing end-to-end preboot security. IPAA can also be used to strengthen unauthorized access prevention during boot to a hard drive.

When encryption is used, performance can be a concern. Encryption algorithms demand a lot of processing power, and if performance slows down noticeably, users may be tempted to store or transmit data in clear formats. Intel-based notebooks, PCs, servers and network components are available with the sheer horsepower needed to run sophisticated applications while encrypting and decrypting data on the fly – with no significant effect on system performance or network throughput. And Intel is always pushing the performance envelope to meet the demands of tomorrow's evermore sophisticated applications and security algorithms.

Communications Security

Mobile PCs are often used to communicate over wireless networks and public Internet connections – as opposed to wired corporate networks that are much easier to protect against intruders. To prevent data tampering as well as eavesdropping, it's important to ensure that connections are always private and secure, no matter where the user travels. Intruders must be prevented from attaching to mobile systems or to the network, either physically or logically, where they could potentially retrieve company-private information, intercept keystrokes, destroy data, plant documents, hijack sessions or deny functionality through malicious code.

In the context of mobile computing, communications security has three dimensions: 1) protecting data stored on the network; 2) protecting remote access from notebook PCs to the network; and 3) ensuring the integrity of the network against intrusion at any point.

Protecting access to the network. This is the crucial step in network security. Strong authentication and key exchange technologies are necessary, but traditional intrusion detection and firewalls also have a role. Authentication should be seen as a prerequisite, which must be followed up with intelligent decisions and actions regarding access control.

An area that is often overlooked but extremely important is the relationship between authentication and the data privacy and integrity keys used to protect communications across the network. If data privacy and integrity keys are not tied in with authentication, then it becomes relatively easy for an attacker to replace a valid communication with a forgery. And the opportunity for forgery or data compromise also grows if these cryptographic keys are not frequently updated.

Mobility exacerbates the problem of key freshness. Ideally, cryptographic keys would expire as soon as an adversary gain controls of the affected platform. To accomplish this, the platform should refresh the cryptographic keys used by the communication system whenever the user, for example, unlocks the screen saver or removes the platform from a suspended state. This means that users must accept the responsibility to password-protect screen savers and similar processes whenever cryptographic keys are present.

Technologies such as VPNs and personal firewalls can supplement traditional techniques to provide excellent access protection. And the industry is continually working to ensure and improve the security of wireless links at both the personal and the network level.

Providing data privacy on the network. This can be accomplished by traditional means, including firewalls, intrusion-detection software, encryption, authentication and more. These methods have long been familiar to IT managers in large organizations, and are increasingly being used in small and mid-sized businesses as deployment costs come down and the ROSI picture becomes more clear.

Internet Protocol Security (IPSec) deserves particular mention as an important addition to corporate firewalls, providing encryption and authentication over public and private networks. This security-standard framework is defined by the Internet

Mobile Security Summary

	Platform Security	Data Protection and System Integrity	Communications Security
Hardware Solutions	Cable locks Motion-detection systems	Biometric authentication (fingerprint reader, voice identification, etc.) Smart cards and USB tokens Intel® Random Number Generator	IPSec-aware hardware IEEE 802.11 WEP (improvement work is ongoing)
Software Solutions	Notebook-tracing software	User IDs and passwords Data encryption	VPN Server and client firewalls
Standards and Specifications	Intel® Protected Access Architecture TCPA trusted platform	TCPA trusted platform	IPSec

Engineering Task Force (IETF), and is designed to provide confidentiality, integrity, and authenticity for data sent over the Internet, extranets, WANs or LANs. Intel supports the IPSec standard, uses IPSec technology on its own Virtual Private Network (VPN), and provides manageable, high-performance IPSec-enabled solutions to every computing segment – from end-user platforms to the corporate LAN and the extended enterprise.

Insuring the integrity of the network against intrusion at any point means identifying the endpoints of each security segment, and armoring those points against intrusion. Many VPN technologies and implementations protect only portions of the communication pathway between mobile PCs and network servers. For example, vulnerability points may exist at the link between the client notebook and the access point, the link between the access point and the ISP, and at various hops along the carrier route between the ISP and the corporate firewall. Not all VPN solutions protect all these links.

One important fact is often misunderstood: In a network, it is infeasible to provide data privacy services without also providing cryptographic integrity services. Encryption fails in this environment unless the design removes the threat of data forgery, including replays of earlier messages. An adversary can use a forgery to attack an encryption algorithm by causing duly authorized equipment to respond to the forgery, implicitly answering questions about the encryption keys.

For maximum security today, the best recommendation is to use VPN in addition to other security methods that are appropriate for your business model and ROSI goals. IPSec-based VPN provides both data privacy and data integrity services, and the design of IPSec ties these back elegantly to an initial authentication and key distribution service. VPN, along with firewalls at both the client and server end of the VPN, provides the optimum protection available today against intrusion anywhere along the access network, no matter what access technology is used.

In addition, it's important to keep up with the latest technologies for secure wireless access. Although vulnerabilities have been found in existing IEEE 802.11 Wired Equivalency Privacy (WEP) implementations, the industry is working diligently to resolve these issues. It will always be a good idea – and is especially important while WEP remains vulnerable – to protect sensitive information by using a VPN with strong user authentication in addition to WEP whenever wireless access is part of your total network topology.

What Intel is Doing about Communications Security

A large portion of the TCPA's specification for trusted computing deals with the authentication of platforms to each other over public and private networks. It can also provide the root for intrusion detection and Firewalling. When you combine platform authentication with server- and client-side firewalls, VPN technology and IPSec, you have all the components to provide a reasonably secure communication environment among all nodes on public and private networks. All these components are available today from Intel.

Security over wireless networks is becoming crucial as well. Intel is a key player in the IEEE 802.11 Task Group i (TGi), which is working to solve security issues in the current WEP security standard, and to enhance wireless LAN security to cover known threats. IEEE 802.11 TGi is working on the enhanced specification. In the meantime, TGi has identified interim solutions that can be used to confidently protect wireless hardware.

In addition to its technical leadership, Intel offers practical help by connecting businesses with leading providers of security products and services through the Intel® e-Business Network – an association of industry partners that includes more than 400 leading independent software developers; 1,800 consultants, integrators and service providers; and over 50,000 channel partners worldwide. To learn more about Intel's e-Business expertise and IeBN leadership, visit www.intel.com/ebusiness.

Companies must devise a multifaceted approach to notebook security in line with their own particular goals. Many companies may determine that their priority will be protecting their data and network security, no matter what may happen to the actual notebook itself.

On the other side of the spectrum, some small companies with less to spend on IT may feel the financial pain involved in lost property more acutely than large companies. While keeping in mind that absolute physical security is impossible, these companies may look toward physical protection as their first and main line of defense.

In either case, companies are advised to create a comprehensive plan for notebook security that includes a cost/benefit analysis to determine which solutions are the best use of money and other limited resources.

– Notebook Security: Protecting Your Property, Data, and Network, An IDC Executive Brief (#203).

Now is the Time, Intel is the Leader

Today's workforce is setting up office in the world at large: at home, in hotels and client sites, on the road, in the air – you name it. The benefits of mobile computing are impossible to ignore. On the other hand, the need for mobile security is something that users and companies ignore at their peril.

Fortunately, mobile security is stronger and easier to implement than ever before at all levels – platform, data, system integrity and communications. And Intel is helping to drive innovations in mobile security by:

- Providing leadership in the TCPA to define the trusted platform, including platform identification and reporting of platform integrity.
- Developing core building-block technologies such as the Intel Protected Access Architecture, Random Number Generator and more, enabling developers to increase the security of their systems and applications.
- Offering support for IPSec, VPN, data encryption and other technologies that secure communications to and from mobile devices, anywhere and anytime.
- Providing processors, chipsets and network components that offer outstanding performance even while processing the most complex security operations.

No matter what security measures you're already taking, it's always wise to re-evaluate and fine-tune them in the light of changing needs and emerging solutions. That's especially true if your business depends on mobile employees who require unconfined access to sensitive data wherever they go. With all that's happening today in the field of mobile security, now is an excellent time to plan your short- and long-term mobile security strategy.

As new threats appear, Intel keeps working on solutions to thwart security concerns.

To Learn More

Visit Intel's security site at http://developer.intel.com/design/security/. There, you'll find a wealth of information covering every level of security, from the network and server level to end-user desktops, mobile PCs and wireless devices. And you'll learn all the ways Intel's products, technology initiatives and alliances can help you create a total security solution that meets your needs as well as your budget.

You can also learn more about newest specifications for trusted computing on the TCPA Web site at www.trustedpc.org. And while you're surfing the Web, check out the Intel e-Business Web site at www.intel.com/ebusiness. It's your doorway to the ideas, products, services and providers that are changing the way e-Business is done – including the mobility and security technologies that are transforming the world into one, big e-Business office place – open to anyone, safe for everyone.

[1] Source: Gartner Consulting, “White Paper: Benefits and TCO of Notebook Computing,” July 19, 2001.

[2] Source: “Upwardly Mobile,” PC Direct, June 2001.

[3] Source: www.safeware.com/losscharts.htm.

[4] Source: IDC Executive Brief #203, “Notebook Security: Protecting Your Property, Data and Network.”

Printed in USA 0202/OC/RC/20K Please Recycle 250365-001